



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,581	12/05/2001	Roy F. Brabson	RSW920010223US1	3407

7590 02/28/2007
Jerry W. Herndon
IBM Corporation T81/503
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER

PAN, JOSEPH T

ART UNIT	PAPER NUMBER
----------	--------------

2135

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/007,581	BRABSON ET AL.	
	Examiner	Art Unit	
	Joseph Pan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 December 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12, 14, 16-18, 20 and 22-39 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12, 14, 16-18, 20 and 22-39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 December 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's response filed on December 12, 2006 has been carefully considered. Claims 1-12, 14, 16-18, 20, 22-39 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-12, 14, 16-18, 20, 22-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anand et al. (U.S. Patent No. 6,141,705), hereinafter "Anand", in view of Freed et al. (US Pub. No. 2003/0014623 A1), hereinafter "Freed".

Referring to claim 1:

i. Anand teaches:

A method of performing security processing in a computing network comprising a local unit having an operating system kernel executing at least one application program, comprising:

receiving a first request at the operating system kernel from the application program to initiate a communication with a remote unit (see figure 3, element 140 'application data'; and column 10, lines 27-47 of Anand);

providing a second request from the operating system kernel to a security offload component which performs security handshake processing, the second request directing the security offload component to secure the communication with the

Art Unit: 2135

remote unit (see e.g. figure 3, element 128 'transport protocol driver, e.g. TCP/IP'; and column 10, lines 27-47 of Anand); and

providing a control function in the operating system kernel for initiating operation of the security handshake processing by the security offload component (see figure 3, element 100 'NIC hardware, e.g. ethernet'; and column 10, lines 27-47 of Anand).

Anand further discloses that "rather than perform certain of the CPU intensive operations on the data packet as it passes through the respective network layers--e.g. checksum calculation/verification, encryption/decryption, message digest calculation and TCP segmentation--those tasks can instead be offloaded and performed at the NIC hardware." (see column 3, lines 39-44 of Anand)

However, Anand does not specifically mention the security handshake processing among the tasks performed by the offload component.

ii. Freed discloses a method for secure communications between a client and a server. The method includes the steps of managing a communication negotiation between the client and the server wherein Freed discloses "Besides authenticating the server to the client, the SSL Handshake Protocol: allows the client and server to negotiate the cipher suite to be used; allows the client and the server to generate symmetric session keys; and establishes the encrypted SSL connection. Once the key exchange is complete, the client and the server use this session key to encrypt all communication between them." (see page 1, paragraph [0008], lines 1-7 of Anand, emphasis added)

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Freed into the system of Anand to offload the security handshake processing to the offload component.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Freed into the system of Anand to offload the security handshake processing to the offload component, because "As such, there is an advantage in offloading such CPU intensive task to a peripheral hardware device. This would reduce processor utilization and memory bandwidth usage in the host computer,

and thereby increase the efficiency, speed and throughput of the overall system.” (see column 2, lines 48-52 of Anand)

Referring to claim 2:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose executing the provided control function, thereby initiating operation of the security handshake processing (see column 10, lines 27-47 of Anand).

Referring to claim 3:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose that the operating system Kernel maintains control over operation of the security handshake processing (see column 10, lines 27-47 of Anand).

Referring to claims 4, 7:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose that kernel does not participate in operation of the security handshake processing (see page 3, paragraph [0034], lines 14-18 of Freed).

Referring to claim 5:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose specifying information to be used by the security offload component (see figure 4, element 150 ‘packet extension’; and column 11, lines 8-27 of Anand).

Referring to claims 6, 8:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the specified information comprises one or more of: a connection identifier; a security role; cipher suites options, etc. (see page 1, paragraphs [0008], [0010] of Freed).

Referring to claims 9, 30:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the completion response from offload component (see page 5, paragraph [0066] of Freed).

Referring to claims 10, 31-32:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the conveyed information comprises one or more of: a session identifier, one or more session keys, a sequence number, a cipher suite, etc. (see page 1, paragraphs [0008], [0010] of Freed).

Referring to claim 11:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose that the operating system kernel maintains control over operation of the security handshake processing, and wherein the operating system kernel provides one or more message segments (see e.g. figure 7, element 237 'Neg. With SSL AD' of Freed).

Referring to claims 12, 14:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the random number generation when creating initial handshake message (see page 4, paragraph [0052] of Freed).

Referring to claims 16-17:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the certificate and decoding (see page 1, paragraph [0009] of Freed).

Referring to claim 18:

Art Unit: 2135

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the encryption (see page 1, paragraph [0009] of Freed).

Referring to claim 20:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the master secret (see page 1, paragraph [0009] of Freed).

Referring to claims 22-23:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the master security secrets and the session cryptography keys (see page 1, paragraphs [0008] – [0009] of Freed).

Referring to claim 24:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the digitally signing (see page 5, paragraph [0054] of Freed).

Referring to claim 25:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose validating a digital certificate (see page 1, paragraph [0009], lines 1-8 of Freed).

Referring to claims 26-29:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose the message authentication code ("MAC") (see page 1, paragraph [0009], last 8 lines of Freed).

Referring to claim 36:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose preparing the data packet, reserving space in the data packet, and passing the data packet to the offload component (see figure 4, element 142 'network packet'; and column 3, lines 39-44 of Anand).

Referring to claims 37-38:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose passing control information from the operating system kernel to the security offload component (see column 4, lines 9-12 of Anand).

Referring to claim 39:

Anand and Freed teach the claimed subject matter: providing a security offload component which performs security handshake, and a control (see claim 1 above). They further disclose encrypting the data in the data packet (see column 9, lines 49-50 of Anand).

Referring to claims 33-35:

i. Anand teaches:

A method of performing security processing in a computing network including a local unit having an operating system kernel executing at least one application program, comprising:

providing a security offload component which performs security session establishment and control processing (see figure 3, element 100 'nic hardware'; column 3, lines 31-44 of Anand);

providing a control function in the operating system kernel for initiating operation of the security session establishment and control processing by the security offload component (see column 3, lines 9-23, lines 61-65; and column 4, lines 9-12 of Anand);

receiving a request at the operating system kernel from the application program to initiate a communication with a remote unit (see figure 3, element 140 'application data' of Anand); and

Art Unit: 2135

directing the security offload component to secure the communication with the remote unit in response to the request (see column 10, lines 27-47 of Anand).

Anand discloses that “rather than perform certain of the CPU intensive operations on the data packet as it passes through the respective network layers--e.g. checksum calculation/verification, encryption/decryption, message digest calculation and TCP segmentation--those tasks can instead be offloaded and performed at the NIC hardware.” (see column 3, lines 39-44 of Anand)

However, Anand does not specifically mention the security session establishment among the tasks performed by the offload component.

ii. Freed discloses a method for secure communications between a client and a server. The method includes the steps of managing a communication negotiation between the client and the server wherein Freed discloses “Besides authenticating the server to the client, the SSL Handshake Protocol: allows the client and server to negotiate the cipher suite to be used; allows the client and the server to generate symmetric session keys; and establishes the encrypted SSL connection. Once the key exchange is complete, the client and the server use this session key to encrypt all communication between them.” (see page 1, paragraph [0008], lines 1-7 of Anand, emphasis added)

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Freed into the system of Anand to offload the security session establishment to the offload component.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Freed into the system of Anand to offload the security session establishment to the offload component, because “As such, there is an advantage in offloading such CPU intensive task to a peripheral hardware device. This would reduce processor utilization and memory bandwidth usage in the host computer, and thereby increase the efficiency, speed and throughput of the overall system.” (see column 2, lines 48-52 of Anand)

Response to Arguments

4. Applicant's arguments filed on December 12, 2006 have been fully considered but are not persuasive.

(1) Applicant argues:

"In distinct contrast, Anand is directed to a system by which security processing is performed by an offload component (e.g. a NIC) under the direction and control of an application program" (see page 2, lines 4-6, Applicant's Arguments/Remarks)

Examiner maintains:

Anand discloses "In a preferred embodiment of the invention, a software implemented method and protocol is provided that allows, for instance, the operating system (OS) to "query" the device drivers (often referred to as "MAC" drivers) of any hardware peripherals (such as a NIC) that are connected to the computer system. The various device drivers each respond by identifying their respective hardware peripheral's processing capabilities, referred to herein as "task offload capabilities." In the preferred embodiment, once the task offload capabilities of each particular peripheral have been identified, the OS can then enable selected peripherals to perform certain tasks that could potentially be used by the OS. The OS can thereafter request that a peripheral perform the previously enabled task, or tasks, in a dynamic, as-needed basis, depending on the then current processing needs of the computer system." (see column 3, lines 9-23 of Anand, emphasis added)

Thus, Anand discloses that the operating system (OS) queries, directs and controls the offload component (e.g. a NIC).

(2) Applicant argues:

"However, element 128 of Anand Figure 3 is explicitly labeled a "Transport Protocol Driver" which a skilled person would necessarily understand to be different from an operating system kernel" (see page 2, last 3 lines, Applicant's Arguments/Remarks)

Examiner maintains:

Anand first discloses that the operating system (OS) **queries, directs and controls** the offload component (e.g. a NIC). (see Examiner's answer in (1) above)

Anand then more specifically discloses "In a preferred embodiment of the present invention, in the Windows NT layered networking architecture, a transport protocol driver, or transport, is implemented with an appropriate program method so as to be capable of **querying** each of the device driver(s) associated with the corresponding NIC(s) connected to the computer." (see column 3, lines 45-50 of Anand, emphasis added).

Thus, Anand discloses that the transport protocol driver, or transport, is implemented in the operating system kernel.

Figure 3 of Anand illustrates that element 128 'transport protocol driver, e.g. TCP/IP' is in the operating system kernel, because it's well known in the art that TCP/IP is in the operating system kernel.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Art Unit: 2135

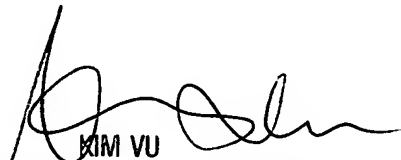
The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-6300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
February 19, 2007


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100